COMPLIANCE BULLETIN

HIGHLIGHTS

While many of the measures introduced by the Digital Privacy Act have been in force since the bill was first enacted in 2015, the government held off on enforcing mandatory breach reporting until the proper regulations were implemented. Such regulations could be in place as early as fall 2017.

Organizations will want to ensure that they know what is expected of them in regards to mandatory data breach notifications in order to remain compliant and avoid costly fines.

Is Your Organization Ready for Mandatory Data Breach Notifications?

OVERVIEW

On June 18, 2015, the Digital Privacy Act (DPA) received royal assent and became law. Among other things, the DPA amended the Personal Information Protection and Electronic Documents Act (PIPEDA) by revising consent requirements, introducing mandatory breach notification and record-keeping requirements, and adding significant fines for non-compliance.

While many of the measures introduced by the DPA have been in force since the bill was first enacted, the government held off on imposing mandatory breach reporting until the proper regulations were implemented.

Such regulations could be in place as early as fall 2017, and organizations will want to ensure that they know what is expected of them in order to remain compliant and avoid costly fines as high as $100,000.

MANDATORY DATA BREACH NOTIFICATIONS

The DPA imposes reporting requirements for every organization in Canada that suffers a data breach, particularly if that data breach creates a real risk of **significant harm** to the personal information of one or more individuals. While the full extent of the reporting

BRYSON INSURANCE

requirements will not be known until the corresponding regulations are published, the DPA defines **significant harm** broadly to include the following:

- Bodily harm
- Humiliation
- Damage to reputations or relationships
- Loss of employment, business or professional opportunities
- Financial loss
- Identity theft
- Negative effects on credit records
- Damage to or loss of property

Most often, the existence of "a real risk of significant harm" will be based on the sensitivity of the personal information involved in the breach, the probability that the personal information will be misused and additional factors that may be prescribed by the forthcoming regulations.

If a breach causing significant harm to one or more individuals occurs, the affected organization must do the following, as soon as feasible:

- ✓ Report the incident to the Office of the Privacy Commissioner of Canada (Privacy Commissioner).
- ✓ Notify affected individuals of the breach and provide them with information on how they may minimize the harm caused by the breach.
- ✓ Inform other organizations and government entities of the breach, especially if they believe that doing so could reduce risks or mitigate harm.

Notices must contain enough information to help affected individuals fully understand the extent of harm caused by the breach. Additionally, notices must be conspicuous and provided directly to affected individuals. However, in limited circumstances, indirect notices may be permitted. Once again, more detail will be available to organizations once the forthcoming regulations are published.

RECORD-KEEPING REQUIREMENTS

Another key change under the DPA will be the requirement that organizations keep records of all security breaches involving personal information. While it is still unclear the level of detail these records will need to contain, it is clear that the Privacy Commissioner will have the right to request and review these records at any time.

PENALTIES FOR NON-COMPLIANCE

Under the DPA, fines up to $100,000 may be imposed against organizations that knowingly violate the mandatory breach notification requirements or breach record-keeping requirements. Until the regulations are finalized, it will remain unclear if a violation will include a single incident (for example, a single failure to notify all individuals impacted by a breach) or each incident (for example, each failure to notify each individual impacted by a breach). However, it is clear that the Privacy Commissioner now has the ability to impose significant fines for non-compliance.

WHAT DOES THIS MEAN FOR ORGANIZATIONS?

Mandatory data breach notifications could impact any organization that is at risk of a cyber attack. Given the reach of the DPA and upcoming regulations, all organizations should consider doing the following:

- Review and update existing protocols and policies to account for detecting, responding and reporting data breach incidents internally.
- Assess the types of information—personal information, intellectual property, supplier data, etc.—they hold and how they would respond in the event of a breach.
- Create a data breach incident response plan if one does not already exist. Such a plan should include methods for notifying the Privacy Commissioner and any impacted individuals.
- Ensure that they have sufficient insurance in place and have taken the steps to mitigate any litigation exposures. Such steps often include requiring employee training, performing security audits and identifying cyber security vendors.

Organizations should review the DPA to ensure they are compliant with all aspects of the legislation. For more information, contact Bryson & Associates Insurance Brokers Ltd today.